REMARKS

Claims 1-36 are pending in the application.

Claims 1-24 and 26-36 are rejected.

Claims 1-24 and 26-36 remain pending in the application.

Applicants respectfully request reconsideration in light of the remarks contained herein.

Claim Rejections - 35 U.S.C. § 103

Claims 1-3, 6-8, 10-12, 14-20, 22-24, 26-30, and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Secure communications Over Insecure Channels," by Ralph C. Merkle, hereinafter *Merkle*, in view of U.S. Patent No. 5,825,890 to Elgamal et al., hereinafter *Elgamal*.

I. The Purported Combination of *Merkle* and *Elgamal* Does Not Disclose Each Element of Claim 1.

"The prior art reference (or references where combined) must teach or suggest all the claim limitations." M.P.E.P. § 2142, 2143. Moreover, "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. All words in a claim must be considered in judging the patentability of that claim against the prior art." M.P.E.P. § 2143.03 (citations omitted).

The Final Office Action states:

> 11. As per claims 1, 6, 14, 28, and 33, Merkle teaches creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token; transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver', randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token; recording in a key escrow database the created set of N trap door encryption decryption function pairs and the corresponding paired token; recording in the key escrow database the randomly selected trap door encryption decryption

> function pair along with the encrypted token; and inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key (pages 296-299).
> 12. Merkle does not disclose adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair.
> 13. Elgamal teaches adding padding information to data prior to encrypting the data (column 17, lines 21-40).

Final Office Action Mailed August 18, 2006 at 4.

1. Elgamal's padding data is not randomization data, as required by the claim.

Applicant respectfully disagrees. Applicant submits that *Merkle* and *Elgamal*, alone or in combination, do not disclose each element of Claim 1. For example, the Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose "adding **randomization information at the receiver** to the corresponding token of the selected trap door encryption-decryption function pair; [and] encrypting the token with the added randomization information at the receiver, the token corresponding with the randomly selected encryption-decryption function pair," as required by Claim 1.

First, Applicant respectfully disagrees that the cited portion of *Elgamal* supplies the above-identified missing elements. The cited portions of *Elgamal* discusses "padding data [that] is used to make the record length be a multiple of the block ciphers block size when a block cipher is used for encryption." *Elgamal*, 17:22-25. *Elgamal*'s "padding data" clearly is not randomization data, as required by the claim.

The Final Office Action states:

> 4. In response to the Applicant's arguments that *Elgamal*'s teaching of padding data is not randomization data as required by the claim, the Examiner disagrees, and it is noted that the features upon which applicant relies, such as the importance of the randomization data, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). According to the claim the combination of the token and the randomization data are encrypted. Additionally, randomizing

> data to be added to a token is unimportant due to the nature of not knowing what data is going to be generated. Furthermore, adding random padding information to keys has been known since at least 09 June 1998 as illustrated by Figures 2-6 and column 9, lines 16-45 of U.S. Patent No. 5,764,772 to Kaufman et al, hereinafter Kaufman.
> 5. Therefore, *Elgamal* discloses the adding the randomization data as claimed by the Applicant and the rejection is maintained.

Final Office Action Mailed August 18, 2006 at 2.

Applicant respectfully notes that the question is not whether the importance of the random information is cited in the rejected claims, but rather whether *Elgamal*'s "padding data" is randomization information. *Elgamal*'s "padding data" clearly is not randomization information, as required by the claim. Elsewhere, *Elgamal* uses the root term "random" a total of twenty-four times to designate which numbers, keys and the like are indeed random. For example, *Elgamal* discusses "randomly generating a number," *id.* at 217:44-45, "the challenge data is a random number to ensure channel integrity," *id.* at 7:16-17, "identification is a randomly generated set of bits," *id.* at 7:23-24, "to generate a new randomized key," *id.* at 10:59-60, and so on for a total of twenty-four uses the root term "random."

Yet, glaringly absent from *Elgamal*'s discussion of "padding data" is any mention of the "padding data" being random. *Elgamal*, 17:29-31. *Elgamal* uses the root term "random" twenty-four times elsewhere, but, with regard to padding data, *Elgamal* makes an obvious distinction. *Elgamal,* therefore does not designate padding data that is random. On the contrary, *Elgamal* says that "[t]he actual value of the padding data is unimportant." *Elgamal*, 17:29-31.

In the implementation discussed in *Elgamal*, the padding data could be a non-random string of ones or zeros. Either of these implementations are in accord with *Elgamal* because "[t]he actual value of the padding data is unimportant," *Elgamal*, 17:29-31. Thus, *Elgamal* does not disclose, teach, or suggest "adding randomization information," as required by the claim.

2. Elgamal, Kaufman, and Merkle de not dislcose adding randomization information at the receiver.

Second, claim 1 requires that the randomization information be added **at the receiver** and that **the receiver encrypt the token with the added randomization information**. *Elgamal*, on the contrary, says that "[t]he **sender** of the 'padded' record appends the padding data." *Elgamal*,

17:26-28 (emphasis added). Thus, *Elgamal* does not disclose, teach, or suggest adding randomization information **at the receiver**, as required by the claim.

The Final Office Action also references U.S. Patent No. 5,764,772 to *Kaufman et al*, hereinafter *Kaufman,* which discusses adding a "pad using the public key of the intended recipient." *Kaufman* at 9:21. Again, *Kaufman* like *Elgamal* says that the padding occurs **before** the data is transmitted to the recipient. *See, e.g., Kaufman* at Fig. 1. *Kaufman* says that "the secret key is encrypted using a public key of the intended recipient and is provided to the intended recipient together with the encrypted message." *Kaufman* at 4:29-33. Furthermore, "[t]he mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of modification." *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780, 1783-84 (Fed. Cir. 1992) (quoting *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988)). The Final Office Action has not cited prior art that suggests desirability of adding randomization information at the receiver. Thus, neither *Elgamal* nor *Kaufman* discloses, teaches, or suggests adding randomization information **at the receiver**, as required by the claim.

Third, the Final Office Action's rationale for the combination of *Merkle* and *Elgamal* similarly fails to compensate for the deficiencies in the references. The Final Office Action cited *Elgamal*, 17:21-40, to show that it would have been obvious to add the missing claim elements. As Applicant has already shown, the cited portion of *Elgamal* does not show adding randomization information, as required by the claim.

II. The Purported *Merkle-Elgamal* Combination Does Not Disclose, Teach, or Suggest Each and Every Element of Applicant's Independent Claims 6, 14, 28, and 33.

The Office Action also relies on the *Merkle-Elgamal* combination to reject independent Claims 6, 14, 28, and 33. Applicant respectfully submits that the proposed *Merkle-Elgamal* combination does not disclose, teach, or suggest each and every element of Applicant's independent claims. Thus, for reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose, teach, or suggest each and every element as set forth in Applicant's independent Claims 6, 14, 28, and 33.

III. There Is No Suggestion or Motivation to Combine *Merkle* with *Elgamal* or *Kaufman*

The question raised under 35 U.S.C. § 103 is whether the prior art taken as a whole would suggest the claimed invention taken as a whole to one of ordinary skill in the art at the time of the invention. *See* 35 U.S.C. § 103(a). Accordingly, even if all elements of a claim are disclosed in various prior art references, which is certainly not the case here as discussed above, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill in the art at the time of the invention would have been prompted to modify the teachings of a reference or combine the teachings of multiple references to arrive at the claimed invention.

"The prior art reference (or references where combined) must teach or suggest all the claim limitations." M.P.E.P. § 2142, 2143. The teaching, suggestion or motivation for the modification or combination and the reasonable expectation of success must both be found in the prior art and cannot be based on an applicant's disclosure. *See id.* (citations omitted). "Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art" at the time of the invention. M.P.E.P. § 2143.01. Even the fact that references *can* be modified or combined does not render the resultant modification or combination obvious unless the prior art teaches or suggests the desirability of the modification or combination. *See id.* (citations omitted). Moreover, "[t]o establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. All words in a claim must be considered in judging the patentability of that claim against the prior art." M.P.E.P. § 2143.03 (citations omitted).

The M.P.E.P. sets forth the strict legal standard for establishing a *prima facie* case of obviousness based on modification or combination of prior art references. To establish a *prima facie* case of obviousness, "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings." M.P.E.P. § 2142, 2143.

The Final Office Action states:

> 14. It would have been obvious to one of ordinary skill in the ad at the time the invention was made to add randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypt the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair, as opposed to sending it back unencrypted as Merkle suggests, since Elgamal discloses at column 17, lines 21-40 that such a modification would allow secure distribution of information by making the intended data the appropriate length for block ciphers, as well as provide a method for the receiver to detect whether the data has been tampered with. Furthermore, adding random padding information to keys has been known since at least 09 June 1998 as illustrated by Figures 2-6 and column 9, lines 16-45 of Kaufman.

Final Office Action Mailed August 18, 2006 at 4.

In response to Applicant's arguments, the Final Office Action states:

> 6. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.26 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation for the combination was provided for at column 17, lines 21-40 of Elgamal. If this motivation were found to be insufficient, one of ordinary skill in the art would generally understand the benefits of adding randomized padding data to key information as again taught by Kaufman in column 9, lines 16-45.

Final Office Action Mailed August 18, 2006 at 2-3.

Even assuming for purposes of argument that the proposed combination discloses the limitations of Applicant's claims, which Applicant disputes, it would not have been obvious to one skilled in the art to make the combination. The cited portions of *Elgamal* and *Kaufman* do not mention "allow[ing] secure distribution of information . . . [or] provid[ing] a method for the receiver to detect whether the data has been tampered with." Final Office Action, at 4-5. Without citation to evidence from the references, this motivation for combination appears to be based on either Applicant's own disclosure or the Office Action's general conclusion that "one of ordinary skill in the art would generally understand the benefits" of the combination. In either

case, the basis of motivation is improper. According to the Federal Circuit, "the deficiencies of the cited references cannot be remedied by . . . general conclusions about what is 'basic knowledge' or 'common sense' to one of ordinary skill in the art." *In re Zurko*, 258 F.3d 1379, 59 USPQ2d 1693, 1679 (Fed. Cir. 2001).

For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claim 1.

IV. The Dependent Claims Are Not Obvious Over the Purported *Merkle-Elgamal* Combination.

Dependent Claims 2 and 3 depend from independent Claim 1, dependent Claims 7, 8, and 10-12 depend from independent Claim 6, dependent Claims 29-30 and 32 depend from independent Claim 28, and dependent claims 34-36 depend from independent Claim 33. Applicant has shown each of the independent claims to be allowable. Accordingly, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 are not obvious over the *Merkle-Elgamal* combination at least because they include the limitations of their respective independent claims.

Additionally, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 recite elements that further distinguish the art. Claim 3 recites "randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token" and "adding randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair." Claims 7, 20, 22, 30, 34, and 36 recite certain similar, though not identical, features and operations. The Final Office Action states:

> 12. As per claims 3, 7, 14, 30 and 36, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n)^2$. Having the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations (page 299).

Final Office Action, page 5.

Applicant disagrees. The Final Office Action does not cite any portion of *Merkle, Elgamal*, or any other evidence to support that "[h]aving the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to

perform more calculations." Applicant is unable to locate any discussion at 299 of "[h]aving the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations." Therefore, the rejection of claims 3, 7, 20, 22, 30, 34, and 36 is improper. For reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose, teach, or suggest the features and operations recited in dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36.

Claims 4, 5, 9, 13, 21, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Merkle*, in view of *Elgamal*., and further in view of U.S. Patent No. 5,815,573 to Johnson, *et al.,* hereinafter *Johnson*. Dependent claims 4 and 5 depend from independent Claim 1, dependent claims 9, 13, and 21 depend from independent Claim 6, and dependent claim 31 depends from independent Claim 28. Applicant has shown that each of the independent Claims are allowable. For at least this reason, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

Additionally, the Final Office Action has not made a *prima facie* showing of obviousness with respect to each of these claims. For example, with respect to claims 4, 5, and 31 the Final Office Action asserts that the combination of *Merkle, Elgamal*, and *Johnson* is motivated because "it would associate a key to a user with provable certainty." Final Office Action, at 8. The Final Office Action, however, does not cite any discussion in *Merkle, Elgamal*, *Johnson*, or any other evidence to support this contention. Similarly, the Final Office Action does not cite any portion of *Merkle, Elgamal*, or *Johnson* to support the motivation contentions with respect to claims 9, 13, and 21. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clear and apparent, Applicant respectfully requests reconsideration and allowance of the pending claims.

Applicant believes no fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

If there are matters that can be discussed by telephone to advance prosecution of this application, Applicant invites the Examiner to contact its attorney at the number provided below.

Respectfully submitted,

Baker Botts L.L.P.
Attorneys for Applicant

/Bradley S. Bowling/_____
Bradley S. Bowling
Reg. No. 52,641

Dated: November 20, 2006

CORRESPONDENCE ADDRESS:

Customer No. 05073